

# Remarks on certain composita of fields

CHRISTIAN U. JENSEN AND ANDERS THORUP

Department of Mathematical Sciences, University of Copenhagen

13 December 2011

**Abstract.** Let  $L$  and  $M$  be two algebraically closed fields contained in some common larger field. It is obvious that the intersection  $C = L \cap M$  is also algebraically closed. Although the compositum  $LM$  is obviously perfect, there is no reason why it should be algebraically closed except when one of the two fields is contained in the other. We prove that if the two fields are strictly larger than  $C$ , and linearly disjoint over  $C$ , then the compositum  $LM$  is not algebraically closed; in fact we shall prove that the Galois group of the maximal abelian extension of  $LM$  is the free pro-abelian group of rank  $|LM|$ , and that the free pro-nilpotent group of rank  $|C|$  can be realized as a Galois group over  $LM$ .

The above results may be considered as the main contribution of this article but we obtain some additional results on field composita that might be of independent interest.

## Introduction.

Let  $L$  and  $M$  be two algebraically closed fields contained in some common larger field. Clearly, the intersection  $C = L \cap M$  is also algebraically closed. Offhand there is no reason why the compositum  $LM$  should be algebraically closed unless one of the fields contains the other. In this paper we show that if  $L$  and  $M$  are proper extensions of  $C$ , and linearly disjoint over  $C$ , then  $LM$  is not algebraically closed (not even separably closed). In particular, if one of the fields  $L$  or  $M$  has transcendence degree 1 over  $C$ , then  $LM$  is not algebraically closed.

The three first sections are basically elementary. Section 1 states as the main observation (Theorem 1.3) that the class of algebraically relatively closed extensions is stable under formation of composita with separably generated extensions. This result plays an essential role in the paper.

Section 2 presents a detailed analysis of  $p$ -socles of field extensions ( $p$  is a given prime) and their relationship to  $p$ -Frattini groups. In addition the section contains a short survey of Kummer theory and Artin–Schreier theory.

Section 3 combines sections 1 and 2 to show that elementary abelian  $p$ -groups up to a certain rank can be realized by an explicit construction as Galois groups over  $LM$  when  $L/C$  and  $M/C$  are proper extensions and linearly disjoint over  $C$ .

Section 4 contains the two main results. For the first one, we use the results on elementary abelian  $p$ -extensions to describe the maximal abelian extension of  $LM$ : Its Galois group is the free pro-abelian group of rank  $|LM|$ .

Finally, for the second main result we use the rather deep Douady–Harbater–Pop theorem on the absolute Galois group of a function field in one variable, and a classical theorem of Witt on  $p$ -extensions of a field of characteristic  $p$ . Combined with the results of Section 3 we show for any prime  $p$  that the free pro- $p$  group of rank  $|C|$  is realizable as a Galois group over  $LM$ . As a consequence, the free pro-nilpotent group of rank  $|C|$  is realizable as a Galois group over  $LM$ .

The precise results, Theorems 4.1 and 4.2 may be considered as the main contribution of this article, but some of the results on field composita in Sections 1 and 3 may be of independent interest.

### Section 1. Auxiliary results on relative algebraic closures of fields.

For the convenience of the reader we recall in this section some concepts and state some elementary results from classical field theory.

**Definitions 1.1.** A subfield  $F$  of the field  $L$  is called *algebraically closed relative to  $L$*  if any element of  $L$  that is algebraic over  $F$  lies in  $F$ , i.e., if  $F$  equals the algebraic closure of  $F$  in  $L$ .

A field extension  $M$  of  $F$  is called *separably generated* if there exists a transcendence basis  $T$  of  $M$  with respect to  $F$  such that  $M$  is an algebraic separable extension of  $F(T)$ .

Recall that two extensions  $L_1/F$  and  $L_2/F$  are called *linearly disjoint* (over  $F$ ) if elements of  $L_2$  that are linearly independent over  $F$  are also linearly independent over  $L_1$ . More symmetrically, the two extensions are linearly disjoint when for any two families  $(x_i)$  in  $L_1$  and  $(y_j)$  in  $L_2$ , both linearly independent over  $F$ , the family of all products  $(x_i y_j)$  is linearly independent over  $F$ . In particular, if  $T$  and  $U$  are two sets of independent variables over  $F$  then  $F(T)$  and  $F(U)$  are linearly disjoint over  $F$  if and only if the union  $S \cup T$  is a set of independent variables over  $F$ .

*Remark 1.2.* Two finite extensions  $L_1/F$  and  $L_2/F$  are linearly disjoint if and only if  $\dim_F L_1 L_2 = (\dim_F L_1)(\dim_F L_2)$ . As a consequence, if the extensions are subfields of a finite Galois extension of  $F$  with Galois group  $G$ , and  $H_1$  and  $H_2$  are the subgroups of automorphisms in  $G$  fixing, respectively,  $L_1$  and  $L_2$ , then the extensions are linearly disjoint if and only if  $G = H_1 H_2$ , where  $H_1 H_2$  is the subset of  $G$  consisting of products  $h_1 h_2$  with  $h_1 \in H_1$  and  $h_2 \in H_2$ .

Finally, assume that one of the two extensions, say  $L_1/F$ , is a Galois extension with group  $G := \text{Gal}(L_1/F)$ . We will make extensive use of the Translation Theorem of Galois theory, see [5, Chapter 12, Theorem 1, p. 115]: The extension  $L_1 L_2/L_2$  is Galois, and restriction of automorphisms defines an injection  $\text{Gal}(L_1 L_2/L_2) \hookrightarrow \text{Gal}(L_1/F)$ . Moreover, the two extensions  $L_1/F$  and  $L_2/F$  are linearly disjoint iff  $L_1 \cap L_2 = F$ , iff the injection of Galois groups is an isomorphism.

The main result in this section is the following.

**Theorem 1.3.** *Let  $M$  and  $L$  be fields contained in some larger field and assume that  $L$  and  $M$  are linearly disjoint over their intersection  $F = M \cap L$ . If  $M$  is a separably generated over  $F$  and  $F$  is algebraically closed relative to  $L$  then  $M$  is algebraically closed relative to the compositum  $ML$ .*

Clearly, to prove the Theorem it suffices to prove it when  $M/F$  is a purely transcendental extension, and when  $M/F$  is an algebraic separable extension. Moreover, it suffices to prove it when  $M/L$  is finitely generated, and we may in fact assume that  $M/F$  is generated by a single element. We separate the proof of the Theorem into the transcendental and the algebraic part.

**Proposition 1.4.** *If  $F$  is a subfield of  $L$  and  $F$  is algebraically closed relative to  $L$ , then the field of rational functions  $F(T)$ , where  $T$  is set of algebraic independent elements over  $L$ , is algebraically closed relative to the field of rational functions  $L(T)$ .*

*Proof.* As noted above we may assume the  $T$  consist of a single element  $t$ , transcendental over  $L$ . Let  $\varphi \in L(t)$ ,  $\varphi \neq 0$ , be algebraic over  $F(t)$ , so there is an equation

$$f_n \varphi^n + \cdots + f_0 = 0 \quad (**)$$

where  $f_i \in F(t)$  and  $f_n \neq 0$ . We must prove that  $\varphi \in F(t)$ .

Multiplying the functions  $f_i$  by a common denominator in  $F[t]$ , we may assume that each  $f_i$  in (\*) is a polynomial in  $F[t]$ . We multiply (\*) by  $f_n^{n-1}$  and obtain an equation of degree  $n$  showing that  $f_n \varphi$  is integral over  $F[t]$ . Since  $\varphi$  lies in  $F(t)$  if  $f_n \varphi$  does, we may assume that  $\varphi$  is integral over  $F[t]$ . In particular,  $\varphi$  is integral over  $L[t]$ , hence  $\varphi$  must lie in  $L[t]$ , because  $L[t]$  being UFD is integrally closed in its quotient field.

Next we show that the coefficients of  $\varphi$  are algebraic over  $F$ . From the assumption that  $F$  is algebraically closed relative to  $L$  it then follows that  $\varphi$  lies in  $F[t]$ .

Let  $\alpha$  be the leading coefficient in  $\varphi$ . By induction on the degree of  $\varphi$  it suffices to show that  $\alpha$  is algebraic over  $F$ . Let  $N$  be highest degree of the polynomials  $f_i \varphi^i$  for  $i = 0, 1, \dots, n$ . Using that the coefficient of  $t^N$  on the left hand side of (\*) is 0 we obtain

$$a_n \alpha^n + \cdots + a_0 = 0$$

where  $a_i$  is the leading coefficient of  $f_i$  if  $f_i \varphi^i$  has degree  $N$  and  $a_i = 0$  otherwise. By the choice of  $N$  at least one  $a_i$  is  $\neq 0$ . Thus  $\alpha$  is algebraic over  $F$ .  $\square$

**Proposition 1.5.** *If  $F$  is a subfield of  $L$  and  $F$  is algebraically closed relative to  $L$  and  $M$  is a finite separable extension of  $F$ , then  $M$  is algebraically closed relative to  $ML$ .*

*Proof.* Since  $M$  is a finite separable extension of  $F$  there exists  $\theta \in M$  such that  $M = F(\theta)$ . We have to show that  $F(\theta)$  is algebraically closed relative to  $L(\theta)$ .

Let  $f \in F[X]$  be the minimal polynomial of  $\theta$  over  $F$ , of degree  $n$  say. Since  $F$  is algebraically closed relative to  $L$ , it follows that  $f$  is irreducible over  $L$ . Thus  $[L(\theta) : L] = [F(\theta) : F] = n$ , and any  $\lambda \in L(\theta)$  can be written

$$\lambda = \ell_0 + \ell_1 \theta + \cdots + \ell_{n-1} \theta^{n-1}. \quad (**)$$

where  $\ell_0, \ell_1, \dots, \ell_{n-1}$  lie in  $L$ .

Assume that  $\lambda$  is algebraic over  $F(\theta)$ . We must show that  $\ell_0, \ell_1, \dots, \ell_{n-1}$  actually lie in  $F$ .

We can write  $f(X) = \prod_{i=1}^n (X - \theta_i)$ , where  $\theta_i$ ,  $1 \leq i \leq n$  (by the separability assumption) are distinct elements in the Galois closure  $M'$  of  $M$ . We may assume that  $\theta = \theta_1$ . For each  $i$ ,  $1 \leq i \leq n$ , there exists an automorphism  $\sigma_i \in \text{Gal}(M'/F)$  such that  $\sigma_i(\theta) = \theta_i$ . Since  $M' \cap L = F$ , the automorphism  $\sigma_i \in \text{Gal}(M'/F)$  extends uniquely to an automorphism (also denoted  $\sigma_i$ ) in  $\text{Gal}(M'L/L)$ , see Remark 1.2,

Clearly for  $1 \leq i \leq n$  we have by (\*\*)

$$\sigma_i(\lambda) = \ell_0 + \ell_1 \theta_i + \cdots + \ell_{n-1} \theta_i^{n-1} \quad (***)$$

Since  $\lambda$  is algebraic over  $F(\theta)$  and  $F(\theta)$  is algebraic over  $F$ , it follows that  $\lambda$  is algebraic over  $F$  and hence root of a non-zero polynomial  $g(t)$  in  $F[X]$ . By applying the automorphism  $\sigma_i$  we conclude that  $\sigma_i(\lambda)$  is also root of  $g(X)$  and hence  $\sigma_i(\lambda)$ ,  $1 \leq i \leq n$ , is algebraic over  $F$ .

Now consider (\*\*\*) as a system of linear equations with  $\ell_0, \dots, \ell_{n-1}$  as unknowns. The determinant of coefficient matrix is the Vandermonde determinant  $\prod_{j>i}(\theta_j - \theta_i)$ , and hence nonzero since the  $\theta_i$ 's are distinct elements of  $M'$ . Consequently each  $\ell_i$  belongs to  $M'$ . Therefore  $\ell_0, \dots, \ell_{n-1}$  are algebraic over  $F$  and thus lie in  $F$ .  $\square$

*Remark 1.6.* The separability assumption in Proposition 1.5 cannot be omitted, as the following example shows. Set  $F_0 = \mathbb{F}_p(a)$  where  $a$  is transcendental. Then  $a \in F_0$  and  $\sqrt[p]{a} \notin F_0$ . Take  $s, t$  algebraically independent over  $F_0$ , and let

$$F = F_0(t), \quad M := F(\sqrt[p]{t}), \quad L := F(s, \sqrt[p]{g}) \text{ where } g = as^p + t.$$

Then  $M/F$  is inseparable. Clearly  $\sqrt[p]{a} \notin M$ , but  $(\sqrt[p]{g} - \sqrt[p]{t})/s = \sqrt[p]{a}$  belongs to the compositum  $LM$ . Hence  $M$  is not algebraically closed relative to  $LM$ . It is a cumbersome computation with  $p$ 'th powers and polynomials in two variables to check that  $F$  is algebraically closed relative to  $L$ .

## Section 2. Socles of field extensions.

We recall some basic concepts and facts from Galois theory. In the following  $p$  always denotes a prime number. The cyclic group of order  $p$  is denoted  $C_p$ . If  $G$  is a group, by a  $G$ -extension of a field  $F$  we mean a Galois extension of  $F$  with  $G$  as Galois group.

By an *elementary abelian  $p$ -extension* of  $F$  we mean a Galois extension whose Galois group is an elementary abelian pro- $p$ -group, that is, a product (finite or infinite) of copies of  $C_p$ .

**Definition 2.1.** For an arbitrary field extension  $L/F$  the  $p$ -socle  $\text{Soc}^p(L/F)$  is defined as the compositum of all  $C_p$ -extensions of  $F$  contained in  $L$ , or, equivalently, as the largest elementary  $p$ -extension of  $F$  contained in  $L$ . (Hence the Galois group of  $\text{Soc}^p(L/F)/F$  is a product of copies of  $C_p$ .)

**Definition 2.2.** Let  $G$  be a finite or a profinite group. The  $p$ -Frattini subgroup  $\Phi^p(G)$  is defined as the intersection of all closed normal subgroups of index  $p$  in  $G$ . The quotient  $G/\Phi^p(G)$  is called the  $p$ -Frattini quotient of  $G$ .

More generally, for a subgroup  $H$  of  $G$  we denote by  $\Phi^p(G, H)$  the intersection of all closed normal subgroups containing  $H$  and of index  $p$  in  $G$ . Equivalently,  $H\Phi^p(G)$  is the intersection of the kernels of all continuous homomorphisms  $\varphi: G \rightarrow C_p$  which are trivial on  $H$ . Clearly,  $\Phi(G, H) = H\Phi(G)$ .

Standard Galois theory immediately implies the following result.

**Proposition 2.3.** Let  $M/F$  be a (not necessarily finite) Galois extension with Galois group  $G$ . The  $p$ -socle of  $M/F$  is the fixed field of the  $p$ -Frattini subgroup  $\Phi^p(G)$ , and the Galois group of  $\text{Soc}^p(M/F)/F$  is the  $p$ -Frattini quotient  $G/\Phi^p(G)$ .

More generally, if  $L \subseteq M$  is the subfield fixed under a subgroup  $H \subseteq G$  then the  $p$ -socle of  $L/F$  is the fixed field of the subgroup  $\Phi^p(G, H)$ .

**Proposition 2.4.** *Let  $L/F$  and  $M/F$  be two (not necessarily finite) Galois extensions for which  $L \cap M = F$ . Then the  $p$ -socle of the compositum  $LM/F$  is the compositum of the  $p$ -socles of  $L/F$  and  $M/F$ .*

*Assume more generally that  $L/F$  and  $M/F$  are separable extensions for which  $L' \cap M = F$ , where  $L'$  is the Galois closure of  $L$ . Then the  $p$ -socle of the compositum  $LM/F$  is the compositum of the  $p$ -socles of  $L/F$  and  $M/F$ .*

*Proof of 2.4 in the Galois case.* If  $L/F$  and  $M/F$  are finite Galois extensions the assertion follows from classical Galois theory, since obviously the  $p$ -Frattini quotient of a product is the product of the  $p$ -Frattini quotients of the factors. For infinite Galois extensions the assertion follows by writing the extensions as directed unions of finite Galois extensions.  $\square$

*Proof of 2.4 in general.* The general result is not used in the proof of our main results, it is more elaborate, and only included for completeness. Also for the general result we may assume that  $L/F$  and  $M/F$  are finite separable extensions. Let  $G$  be the Galois group of a Galois extension of  $F$  containing  $LM$ . Then the extension contains  $L'M$ , and the subfields  $L \subseteq L'$ , and  $M$ , correspond to subgroups, say,  $N \supseteq N'$  and  $H$  of  $G$ . Clearly  $LM$  corresponds to subgroup  $N \cap H$ . The subset  $N'H \subseteq G$  is a subgroup since  $N'$  is normal; it corresponds to the intersection  $L' \cap M$  which equals  $F$  by assumption. Hence  $N'H = G$ . In particular,  $NH = G$ , that is, any  $g \in G$  has a factorization,

$$g = nh \text{ where } n \in N, h \in H.$$

We use the factorizations to define, for any homomorphism  $\varphi: G \rightarrow C_p$  which is trivial on  $N \cap H$ , two maps  $\varphi_N, \varphi_H: G \rightarrow C_p$  such that

$$\varphi_N(g) = \varphi(n), \varphi_H(g) = \varphi(h) \quad \text{when } g = nh, n \in N, h \in H.$$

First, the maps  $\varphi_N, \varphi_H$  are well defined since  $\varphi$  is a homomorphism trivial on  $N \cap H$ . Clearly  $\varphi(g) = \varphi_H(g)\varphi_N(g)$ . Next, it is obvious that  $\varphi_N$  equals 1 on  $H$  and  $\varphi_H$  equals 1 on  $N$ . We show at the end of the proof that the two maps  $\varphi_N, \varphi_H: G \rightarrow C_p$  are group homomorphisms.

Now the equation of  $p$ -socles is equivalent to the following equation of relative  $p$ -Frattini subgroups:

$$\Phi^p(G, N \cap H) = \Phi^p(G, N) \cap \Phi^p(G, H). \quad (*)$$

As  $\Phi^p(G, N)$  is the intersection of the kernels of all homomorphisms  $\psi: G \rightarrow C_p$  trivial on  $N$ , it is obvious that the inclusion “ $\subseteq$ ” holds in (\*).

To prove the reverse inclusion “ $\supseteq$ ”, let  $g$  be an element on the right side of (\*). We have to prove that  $g$  belongs to the left side, that is,  $\varphi(g) = 1$  for every homomorphism  $\varphi: G \rightarrow C_p$  which is trivial on  $N \cap H$ . Use the above decomposition  $\varphi = \varphi_N \varphi_H$  where  $\varphi_N$  is trivial on  $H$  and  $\varphi_H$  is trivial on  $N$ . As shown below, the maps are homomorphisms  $\varphi_N, \varphi_H: G \rightarrow C_p$ . Therefore, since  $g$  belongs to the right hand side we have  $\varphi_N(g) = 1$  and  $\varphi_H(g) = 1$ . Consequently  $\varphi(g) = \varphi_N(g)\varphi_H(g) = 1$ , as asserted.

It remains to prove that the maps  $\varphi_N$  and  $\varphi_H$  are group homomorphisms. So let  $g, g' \in G$  and write  $g = nh, g' = n'h'$  with  $n, n' \in N$  and  $h, h' \in H$ . As

noticed in the very beginning of the proof we have even  $G = N'H$ ; in particular we may assume that  $n_2 \in N'$ . Now use the equation,

$$g_1g_2 = n_1h_1n_2h_2 = (n_1h_1n_2h_1^{-1})(h_1h_2).$$

Here  $h_1h_2 \in H$ , and  $n_1h_1n_2h_1^{-1} \in N$ , since  $\tilde{N}$  is normal and  $N' \subseteq N$ . Hence

$$\varphi_H(g_1g_2) = \varphi(h_1h_2) = \varphi(h_1)\varphi(h_2) = \varphi_H(g_1)\varphi_H(g_2).$$

Similarly, since  $\varphi_N$  takes values in a commutative group, it follows that  $\varphi_N$  is a homomorphism.  $\square$

**Example 2.5.** Clearly the assumption  $L' \cap M = F$  in 2.4 is stronger than assuming that  $L/F$  and  $M/F$  are linearly disjoint. The stronger assumption is only used at the very end of the proof to justify that the maps  $\varphi_N$  and  $\varphi_H$  are homomorphisms. The authors haven't been able to decide whether the conclusion in 2.4 holds under the simpler assumption that  $L/F$  and  $M/F$  are linearly disjoint. In the following example the two extensions are not linearly disjoint.

Let  $F := \mathbb{Q}(\varepsilon_p)$ , where  $\varepsilon_p$  is a primitive  $p$ 'th root of unity. Choose a prime  $q$  such that  $q \equiv 1 \pmod{p}$ , and let  $L_1 := F(\sqrt[q]{2})$  and  $L_2 = F(\varepsilon_q \sqrt[q]{2})$ . Clearly  $L_1 \cap L_2 = F$ . The extensions  $L_1/F$  and  $L_2/F$  have degree  $q$ , and hence their  $p$ -socles are trivial:  $\text{Soc}^p(L_1/F) = \text{Soc}^p(L_2/F) = F$ . However, the compositum  $L_1L_2$  contains the field  $F(\varepsilon_q)$  which is a  $C_{q-1}$ -extension of  $F$ . So there is a unique  $C_p$ -extension of  $F$  contained in  $F(\varepsilon_q)$ . In particular, the  $p$ -socle of  $L_1L_2/F$  is nontrivial.

However, the  $p$ -socle of  $L_1L_2/F$  is nontrivial. Indeed, the compositum  $L_1L_2$  contains the field  $F(\varepsilon_q)$  which is a  $C_{q-1}$ -extension of  $F$ . So there is a unique  $C_p$ -extension of  $F$  contained in  $F(\varepsilon_q)$ .

**Proposition 2.6.** *Assume that  $E/F$  is contained in a Galois  $p$ -extension  $N/F$ . If  $\text{Soc}^p(E/F) = F$ , then  $E = F$ .*

*Proof.* The assertion translates into the well-known property of  $p$ -Frattini subgroups of a  $p$ -group: If  $H \subseteq G$  is an inclusion of  $p$ -groups, such that  $H\Phi^p(G) = G$  then  $H = G$ .  $\square$

**Corollary 2.7.** *Let  $N/F$  be a Galois  $p$ -extension and  $K/F$  an arbitrary extension. If  $\text{Soc}^p(N/F) \cap K = F$  then  $N \cap K = F$ .*

*Proof.* Use the previous Proposition with  $E := N \cap K$ .  $\square$

*Remarks on Kummer extensions and Artin-Schreier extensions 2.8.* We fix a field  $F$  and distinguish between the case, where the characteristic of  $F$  is  $\neq p$  and the case where the characteristic of  $F$  is  $p$ .

In the first case we will assume that  $F$  contains the  $p$ -th roots of unity. In this situation any  $C_p$ -extension is a Kummer extension  $F(\sqrt[p]{a})$ ,  $a \in F^*$ . Here  $\sqrt[p]{a}$ , being a root of  $X^p - a$ , is only determined up to factor  $\zeta$  where  $\zeta$  is a  $p$ -th root of unity, but since  $F$  contains  $\zeta$  the corresponding root fields coincide.

For a subset  $A \subseteq F^*$  we denote by  $F(\sqrt[p]{A})$  the extension generated by all elements  $\sqrt[p]{a}$  for  $a \in A$ . In particular, for an extension  $L/F$  we have  $\text{Soc}^p(L/F) = F(\sqrt[p]{A})$  where  $A = (L^*)^p \cap F$ . We shall need the following observations: If  $a_1, \dots, a_n$  are elements of  $F^*$ , then the extension  $F(\sqrt[p]{a_1}, \dots, \sqrt[p]{a_n})/F$  has Galois group  $C^n$  if

and only if the classes of the  $a_i$  in the (multiplicative) group  $F^*/(F^*)^p$  are linearly independent over  $\mathbb{F}_p$ , that is, if the relation,

$$a_1^{\nu_1} \cdots a_n^{\nu_n} \in (F^*)^p,$$

implies that  $\nu_i \equiv 0 \pmod{p}$ ,  $1 \leq i \leq n$ . Also, if  $A$  is a subset of  $F^*$ , and  $b \in F^*$ , then  $\sqrt[p]{b} \in F(\sqrt[p]{A})$  if and only if the class of  $b$  in group  $F^*/(F^*)^p$  belongs to the subgroup generated by the classes of the elements of  $A$ .

With a similar notion in characteristic  $p$  we have the following observations: Any  $C_p$ -extension of  $F$  is an Artin–Schreier extension  $F(\wp^{-1}a)$ . Here  $\wp(X) = X^p - X$  and  $\wp^{-1}a$ , denoting a root of  $X^p - X - a$ , is only determined up to addition of a constant  $c \in \mathbb{F}_p$ . but the root fields coincide.

For an extension  $L/F$  we have  $\text{Soc}^p(L/F) = F(\wp^{-1}A)$  where  $A = \wp(L) \cap F$ . If  $a_1, \dots, a_n$  are elements of  $F$ , then the extension  $F(\wp^{-1}a_1, \dots, \wp^{-1}a_n)/F$  has Galois group  $C_p^n$  if and only if the classes of the  $a_i$  in the (additive) group  $F/\wp(F)$  are linearly independent over  $\mathbb{F}_p$ . Also, if  $A$  is a subset of  $F$ , and  $b \in F$ , then  $\wp^{-1}b \in F(\wp^{-1}A)$  if and only if the class of  $b$  in group  $F/\wp(F)$  belongs to the subgroup generated by the classes of the elements of  $A$ .

*Remarks on maximal abelian extensions 2.9.* Denote by  $G_F$  the Galois group of the separable closure of  $F$ , and by  $G_F^{\text{ab}}$  the Galois group of the maximal abelian extension of  $F$ . In addition, denote by  $G_F(p)$  and  $G_F^{\text{ab}}(p)$  the maximal pro- $p$  quotient groups. Thus  $G_F^{\text{ab}}(p)$  is the Galois group of the maximal abelian  $p$ -extension of  $F$ .

Assume the  $F$  contains all  $n$ 'th roots of unity for exponents  $n$  not divisible by the characteristic of  $F$ . Then the group  $G_F^{\text{ab}}(p)$  is a free pro-abelian  $p$ -group, determined by the formula:

$$G_F^{\text{ab}}(p) = \hat{\mathbb{Z}}_p^{I_p} \text{ where } |I_p| = \begin{cases} \text{rank}_{\mathbb{F}_p} F^*/(F^*)^p & \text{if } p \neq \text{Char}(F), \\ \text{rank}_{\mathbb{F}_p} F/\wp(F) & \text{if } p = \text{Char}(F), \end{cases} \quad (*)$$

where  $\hat{\mathbb{Z}}_p$  is the (additive) group of  $p$ -adic integers. Indeed, assume first that  $p \neq \text{Char}(F)$ . Then Kummer theory may be combined with a theorem of Capelli [1], see also [5]. Accordingly, if  $a \in K^*$  and  $a \notin (K^*)^p$ , then the  $i$ 'th field in the tower,

$$F \subset F(\sqrt[p]{a}) \subset \cdots \subset F(\sqrt[p^i]{a}) \subset \cdots,$$

is a cyclic extension of  $F$ , and it is of degree  $p^i$  by Capelli. Consequently, the union of the fields in the tower is a  $\hat{\mathbb{Z}}_p$ -extension of  $F$ . It follows easily that the Galois group  $G_F^{\text{ab}}(p)$  is the free pro-abelian  $p$ -group of rank equal to the rank of  $F^*/(F^*)^p$  as a vector space over  $\mathbb{F}_p$ , that is, the formula in the first case holds.

The formula in the second case follows from the theorem of Witt: The Galois group  $G_F(p)$  of the maximal  $p$ -extension of  $F$  is the free pro- $p$ -group of rank equal to the rank of  $F/\wp(F)$ . Hence its maximal abelian quotient is a free pro-abelian group of the same rank.

It follows from the formula that the Galois group  $G_F^{\text{ab}}$  of the maximal abelian extension of  $F$  is the pro-abelian group,

$$G_F^{\text{ab}} = \prod_p \mathbb{Z}_p^{I_p},$$

where the product is over all primes  $p$  and the cardinality of  $I_p$  is given by  $(*)$ .

### Section 3. Constructions of elementary abelian $p$ -extensions.

In this section we fix an algebraically closed field  $C$ , and we let  $T$  and  $U$  be two nonempty subsets of a set of independent variables over  $C$ . We work inside a large algebraically closed field containing the rational function field  $C(T, U)$ , and consider the separable closures  $\widetilde{C(T)}$  and  $\widetilde{C(U)}$ , where separable closure has been indicated with a tilde. We show that the compositum  $\widetilde{C(T)}\widetilde{C(U)}$  of  $\widetilde{C(T)}$  and  $\widetilde{C(U)}$  is not separably closed and that any finitely generated pro-nilpotent group and that any elementary abelian  $p$ -group of rank at most the maximum of  $|C|$ ,  $|T|$ , and  $|U|$ , is realizable as Galois group over the compositum. We proceed in a series of lemmas.

**Lemma 3.1.** *The intersection  $\widetilde{C(T)} \cap C(T)\widetilde{C(U)}$  equals  $C(T)$ .*

*Proof.* The field  $C$  is algebraically closed, and in particular algebraically closed relative  $\widetilde{C(U)}$ . By Proposition 1.4,  $C(T)$  is algebraically closed relative to  $C(T)\widetilde{C(U)}$ . In particular, if an element of  $C(T)\widetilde{C(U)}$  is separably algebraic over  $C(T)$  then it belongs to  $C(T)$ .  $\square$

**Lemma 3.2.** *The intersection  $\widetilde{C(T)}C(U) \cap C(T)\widetilde{C(U)}$  equals  $C(T, U)$ .*

*Proof.* Consider the following diagram of fields and inclusions:

$$\begin{array}{ccccc} \widetilde{C(T)} & \subseteq & \widetilde{C(T)}C(U) & \subseteq & \widetilde{C(T)}\widetilde{C(U)} \\ \cup & & \cup & & \cup \\ C(T) & \subseteq & C(T, U) & \subseteq & C(T)\widetilde{C(U)}. \end{array} \quad (\dagger)$$

To facilitate the notation, we let  $L_0 := C(T)$ ,  $M_0 := C(U)$ ,  $F := C(T, U)$ ,  $M := C(T)\widetilde{C(U)}$  and we let  $L := \widetilde{C(T)}C(U) = \tilde{L}_0 M_0$ . Then the fields of the above diagram are the following:

$$\begin{array}{ccccc} \tilde{L}_0 & \subseteq & L & \subseteq & LM \\ \cup & & \cup & & \cup \\ L_0 & \subseteq & F & \subseteq & M \end{array}, \quad (\ddagger)$$

and  $LM = \tilde{L}_0 \tilde{M}_0$ . Consider the vertical extensions. The first is Galois; its Galois group  $G_0 := \text{Gal}(\tilde{L}_0/L_0)$  is the absolute Galois group of  $L_0$ . Therefore, by the Translation Theorem, see [5], the next two vertical extensions are also Galois, and for the Galois groups  $G := \text{Gal}(L/F)$  and  $G' := \text{Gal}(LM/M)$  we have injections,

$$G_0 \hookleftarrow G \hookleftarrow G'.$$

The inclusion  $G' \rightarrow G_0$  is surjective if and only if  $\tilde{L}_0 \cap M = L_0$ . Hence, by Lemma 3.1, the inclusion  $G' \rightarrow G_0$  is an isomorphism. Therefore, so is the inclusion  $G' \rightarrow G$ . Hence, again by the Translation Theorem, we have the equation  $L \cap M = F$ , which is the asserted equality.  $\square$

**Lemma 3.3.** *For the given prime  $p$  we have the following equation of  $p$ -socles:*

$$\text{Soc}^p(\widetilde{C(T)}\widetilde{C(U)}) / C(T, U) = \text{Soc}^p(\widetilde{C(T)}) / C(T) \cdot \text{Soc}^p(\widetilde{C(U)}) / C(U)$$



*Proof.* We use the same notation as in the previous proof, and refer to the diagram  $(\ddagger)$ . By the previous Lemma, the Galois group  $G = \text{Gal}(L/F)$  equals  $G_0 = \text{Gal}(\tilde{L}_0/L_0)$ , the absolute Galois group of  $L_0$ . So the two groups have the same  $p$ -Frattini quotients. Consequently, for the  $p$ -socle we obtain the first of the following equations,

$$\begin{aligned} \text{Soc}^p(L/F) &= \text{Soc}^p(\tilde{L}_0/L_0)F, \\ \text{Soc}^p(M/F) &= \text{Soc}^p(\tilde{M}_0/M_0)F. \end{aligned} \quad (*)$$

The second equation follows from the symmetry in  $T$  and  $U$ .

Finally, by Proposition 2.4, the  $p$ -socle of  $LM/F$  is the compositum of the  $p$ -socles of  $L/F$  and  $M/F$ , or, by the equations  $(*)$ ,

$$\text{Soc}^p(LM/F) = \text{Soc}^p(\tilde{L}_0/L_0) \text{Soc}^p(\tilde{M}_0/M_0).$$

The latter equation is the asserted equality of socles.  $\square$

**Lemma 3.4.** *Assume that  $p \neq \text{Char } C$ . Fix  $t \in T$  and  $u \in U$ , and consider the field  $C(t+u)$ . Take any  $n$  distinct elements  $c_1, \dots, c_n \in C$ . Then the following extension:*

$$C(t+u)(\sqrt[p]{t+u+c_1}, \dots, \sqrt[p]{t+u+c_n})$$

*is an elementary abelian  $p$ -extension of  $C(t+u)$  with Galois group  $C_p^n$ , and linearly disjoint with  $\widetilde{C(T)}\widetilde{C(U)}$  over  $C(t+u)$ .*

*Proof.* For simplicity, set  $q_i := t+u+c_i$ ,  $i = 1, \dots, n$ . It suffices to prove that the  $n$  roots  $\sqrt[p]{q_1}, \dots, \sqrt[p]{q_n}$  generate over  $\widetilde{C(T)}\widetilde{C(U)}$  an elementary abelian  $p$ -extension with group  $C_p^n$ . The polynomials  $q_i$  belong to the field  $C(T, U)$ , and by the remarks on Kummer theory in 2.8, it suffices to prove that the classes of the  $q_i$  modulo the multiplicative subgroup of  $C(T, U)^*$  describing the  $p$ -socle of  $\widetilde{C(T)}\widetilde{C(U)}$  over  $C(T, U)$  are linearly independent over  $\mathbb{F}_p$ . The  $p$ -socle is described in Equation  $(\ddagger)$  in Lemma 3.3, and the socles on the right hand side of the equation are the maximal elementary abelian  $p$ -extensions of  $C(T)$  and  $C(U)$ . Hence it suffices to show for any equation of the following form in  $C(T, U)^*$ :

$$q_1^{\nu_1} \cdots q_n^{\nu_n} = \varphi \psi \alpha^p \quad (\text{with } \nu_i \in \mathbb{Z}), \quad (**)$$

where  $\varphi \in C(T)^*$ ,  $\psi \in C(U)^*$  and  $\alpha \in C(T, U)^*$ , that  $\nu_i \equiv 0 \pmod{p}$  for  $i = 1, \dots, n$ . To prove it, fix  $i$ , and let  $v: C(T, U)^* \rightarrow \mathbb{Z}$  be the  $q_i$ -adic valuation. Then  $v(q_j) = 0$  for  $j \neq i$ , and  $v(q_i) = 1$ . So the value of  $v$  on the left of  $(**)$  is  $\nu_i$ . On the right, the value of  $v$  at  $\varphi$  and  $\psi$  is zero, since  $q_i$  does not belong to  $C(T)$  or to  $C(U)$ . Hence the value on the right side is a multiple of  $p$ . Therefore  $\nu_i \equiv 0 \pmod{p}$ .  $\square$

**Proposition 3.5.** *Any elementary abelian pro- $p$ -group of rank at most the maximum of  $|C|$ ,  $|T|$ ,  $|U|$ , can be realized as a Galois group over the compositum  $\widetilde{C(T)}\widetilde{C(U)}$ .*

*Proof.* Assume first that  $p \neq \text{Char } C$ . Then Lemma 3.4 applies. Varying  $n$  it follows first that we may realize  $C_p^{|C|}$  over the compositum, and varying similarly  $t \in T$  and  $u \in U$  we may realize all elementary abelian pro- $p$ -groups of the asserted rank.

The case  $p = \text{Char } C$  remains. Only the first part of the proof of Lemma 3.4 needs to be changed. Take any  $t \in T$ ,  $u \in U$ , and set  $q := t + u$ . Let  $c_1, \dots, c_n$  be any  $n$  elements of  $C$  linearly independent over the prime field  $\mathbb{F}_p$ . We prove that the  $n$  roots  $\wp^{-1}(c_1/q), \dots, \wp^{-1}(c_n/q)$  generate an elementary abelian  $p$ -extension of  $\widetilde{C(T)}\widetilde{C(U)}$  with Galois group  $C_p^n$ . Using the description of the  $p$ -socle in Lemma 3.4, and the remarks on Artin–Schreier theory in 2.8 it suffices to show for any equation of the following form in  $C(T, U)$ :

$$\nu_1 c_1/q + \dots + \nu_n c_n/q = \varphi + \psi + \alpha^p - \alpha \quad (\text{with } \nu_i \in \mathbb{Z}),$$

where  $\varphi \in C(T)$ ,  $\psi \in C(U)$  and  $\alpha \in C(T, U)$ , that  $\nu_i \equiv 0 \pmod{p}$  for  $i = 1, \dots, n$ . It suffices to prove that the equation implies that the numerator  $c = \nu_1 c_1 + \dots + \nu_n c_n$  on the left side vanishes. Assume that  $c \neq 0$ . Then the value of the  $q$ -adic valuation on the left side equals  $-1$ . On the right side the value is zero or  $+\infty$  at  $\varphi$  and at  $\psi$ . Hence a contradiction is obtained since no discrete valuation can take the value  $-1$  at an element of the form  $\alpha^p - \alpha = \alpha(\alpha^{p-1} - 1)$ .  $\square$

#### Section 4. Realization of Galois groups over the compositum.

In this section we consider two algebraically closed fields  $L$  and  $M$  contained in some common larger algebraically closed field. We assume that none of the two fields is contained in the other, and we assume that  $L$  and  $M$  are linearly disjoint over their intersection  $C = L \cap M$ . Clearly the intersection  $C$  is algebraically closed. We show that the compositum  $LM$  is not separably closed and, moreover, we show that any pro-nilpotent group with a generating set of cardinality at most  $|C|$  is realizable as a Galois group over  $LM$ . In addition, any elementary abelian  $p$ -group with a generating set of cardinality at most the maximum of  $|L|$  and  $|M|$  is realizable over  $LM$ .

Since  $C$  is perfect, we can choose separating transcendence bases  $T$  for  $L/C$  and  $U$  for  $M/C$ , see [9, Theorem 31, p. 105]. Both are non-empty since  $C$  is strictly contained in  $L$  and  $M$ . Moreover, since  $L/C$  and  $M/C$  are linearly disjoint, it follows from the observations in Remark 1.2 that the union  $T \cup U$  is algebraically independent over  $C$ . So the setup of Section 3 applies:  $L = \widetilde{C(T)}$  and  $M = \widetilde{C(U)}$ , except that the two fields were denoted  $\tilde{L}_0$  and  $\tilde{M}_0$  in Lemma 3.2. Clearly the maximum of  $|C|$ ,  $|T|$ , and  $|U|$  is equal to the maximum of  $|L|$  and  $|M|$ , and hence equal to  $|LM|$ .

**Theorem 4.1.** *Let  $L$  and  $M$  be algebraically closed fields, of which none is contained in the other, and linearly disjoint over their intersection  $C := L \cap M$ . Let  $N := LM$  be their compositum. Then the Galois group  $G_N^{\text{ab}}$  of the maximal abelian extension of  $N$  is the free pro-abelian group of rank  $|N|$ , that is,  $G_N^{\text{ab}} \simeq \hat{\mathbb{Z}}^N$ .*

*Proof.* All roots of unity belong to  $N$  since  $N$  contains an algebraically closed field. Hence it follows from the remarks in 2.9 that  $G_N^{\text{ab}}(p)$  is a free pro-abelian  $p$ -group and that its rank is given by the formula (\*) is 2.9. In the notation above  $N = \widetilde{C(T)}\widetilde{C(U)}$ . Hence it follows from 3.5 that the rank is at least the maximum of  $|C|$ ,  $|T|$ , and  $|U|$ , and hence at least equal to  $|N|$ . Consequently, the rank is equal to  $|N|$ , that is,  $G_N^{\text{ab}}(p) = \hat{\mathbb{Z}}_p^N$ . Therefore, by formula (‡) in 2.9,  $G_N^{\text{ab}} = \hat{\mathbb{Z}}^N$ , and the theorem has been proved.  $\square$

**Theorem 4.2.** *In the setup of Theorem (4.1) the free pro- $p$ -group of rank  $|C|$  is realizable as Galois group over the compositum  $N = LM$ . As a consequence, the free pro-nilpotent group of rank  $|C|$  is realizable.*

*Proof.* Fix from the separating transcendency bases elements  $t \in T$  and  $u \in U$ , let  $K$  be the maximal  $p$ -extension of  $C(t+u)$ , and denote by  $G(p)$  the Galois group of  $K/C(t+u)$ .

Assume first that  $p \neq \text{Char } C$ . Let  $S$  be the  $p$ -socle of  $K/C(t+u)$ . The polynomials  $t+u+c$ ,  $c \in C$ , generate the multiplicative group  $C(t+u)^*$  (up to multiplication by a constant in  $C^*$ ), since  $C$  is algebraically closed. Hence, by Kummer theory,  $S$  is the maximal extension of the form in Lemma 3.4. The latter extension is linearly disjoint with  $N$  over  $C(t+u)$  by Lemma 3.4. So the subfield  $S$  is linearly disjoint with  $N$  over  $C(t+u)$ . Finally, by Proposition 2.6,  $K$  is linearly disjoint with  $N$  over  $C(t+u)$ . Consequently  $\text{Gal}(KN/N) = \text{Gal}(K/C(t+u)) = G(p)$ . Finally, it follows from the Douady–Harbater–Pop theorem on the absolute Galois group of the function field  $C(t+u)$  (see [2],[3],[6], or Haran–Jarden [4] for an easily accessible proof) that  $G(p)$  is the free pro- $p$  group of rank  $|C|$ .

If  $p = \text{Char}(C)$ , we use the Theorem of Witt [8] (see also J.-P. Serre [7, Corollaire 1, p. 91]) on the maximal  $p$ -extension of a field of characteristic  $p$ . Accordingly, the maximal Galois  $p$ -extension of  $N$  is a free pro- $p$ -group  $G_N(p)$  of rank equal to the rank of  $N/\wp(N)$ . It follows from Proposition 3.5 that  $|N/\wp(N)| \geq |C|$ . Consequently, the free pro- $p$  group of rank  $|C|$  is a quotient of  $G_N(p)$ , and hence realizable over  $N$ .

Thus the first assertion has been proved for all  $p$ . Clearly the last assertion is a consequence since a pro-nilpotent group is the over all primes  $p$  of pro- $p$  groups, and hence realizable by the compositum of the fields realizing the factors.  $\square$

*Note 4.3.* Given the algebraically closed fields  $L$  and  $M$  none of which is contained in the other so that  $C = L \cap M$  is properly contained in them both. It is part of the results in Section 3 that  $L/C$  and  $M/C$  are linearly disjoint if and only if the union  $T \cup U$  of the separating transcendency bases is algebraically independent over  $C$ . The condition of being linearly disjoint over  $C$  is clearly equivalent to the condition on the separating transcendency bases  $T$  and  $U$  that their union  $T \cup U$  is algebraically independent over  $C$ .

The authors have not been able to decide if the condition of linear disjointness is always satisfied. It is clearly satisfied if one of  $T$  and  $U$  is a singleton. As a consequence, the conclusions in 4.1 and 4.2 hold if  $L$  or  $M$  has transcendence degree 1 over  $C$ .

## REFERENCES

- [1] A. Capelli, *Sulla riduttibilità della funzione  $x^n - A$  in un campo qualunque di razionalità*, Math. Ann. **54** (1901), 602–603.
- [2] A. Douady, *Détermination d'un groupe de Galois*, C. R. Acad. Sci. Paris **258** (1964), 5305–5308.
- [3] D. Harbater, *Fundamental groups and embedding problems in characteristic  $p$* , Recent developments in the inverse Galois problem, M. Fried, et al., eds, AMS Contemp. Math., vol. 186, 1995, pp. 353–369.
- [4] D. Haran and M. Jarden, *The absolute Galois group of  $C(x)$* , Pacific J. Math. **196** (2000), 445–459.
- [5] F. Lorenz, *Algebra Volume I: Fields and Galois Theory*, Universitext, Springer, 2006.
- [6] F. Pop, *Étale Galois covers of affine smooth curves. The geometric case of a conjecture of Shafarevich*, Algebraic Number Theory, J. Reine Math. **122** (1995), 555–573.

- [7] J.-P. Serre, *Cohomologie Galoisienne*, Lecture Notes in Mathematics 5, Springer, Berlin, 1973.
- [8] E. Witt, *Konstruktion von galoisschen Körpern der Charakteristik  $p$  zu vorgegebener Gruppe der Ordnung  $p^f$* , J. Reine Angew. Math. **174** (1936), 237–245.
- [9] O. Zariski and P. Samuel, *Commutative Algebra Volume I*, with the cooperation of I. S. Cohen, University series in higher mathematics, Van Nostrand Company, Princeton, New Jersey, 1958.

UNIVERSITETSPARKEN 5, DK-2100 COPENHAGEN, DENMARK  
*E-mail address:* `cujensen@math.ku.dk`, `thorup@math.ku.dk`